

# 苏州大学实验报告

院、系	计算机学院	姓名	朱金涛	学号	2327406014
课程名称	计算机网络				
指导教师	高国举		实验完成日期	2025年12月2日	

实验名称： ICMP 和 IGMP

## 一、 实验目的

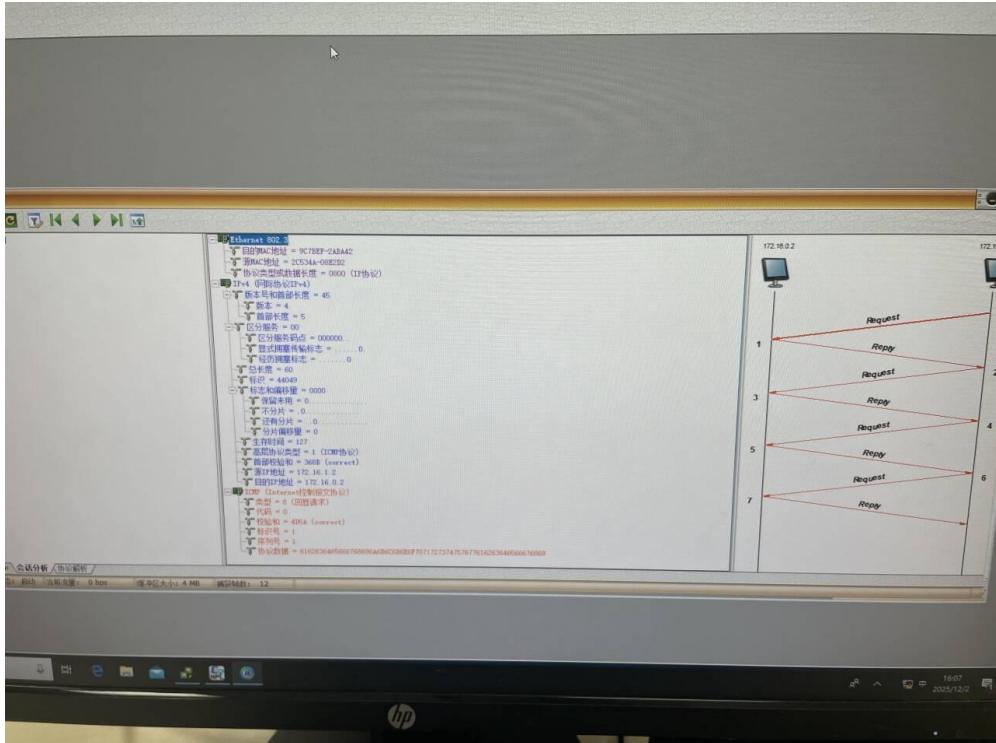
- 掌握 ICMP 协议的报文格式
- 理解不同类型 ICMP 报文的具体意义
- 了解常见的网络故障
- 了解 IGMP 的工作原理

## 二、 实验步骤与结果

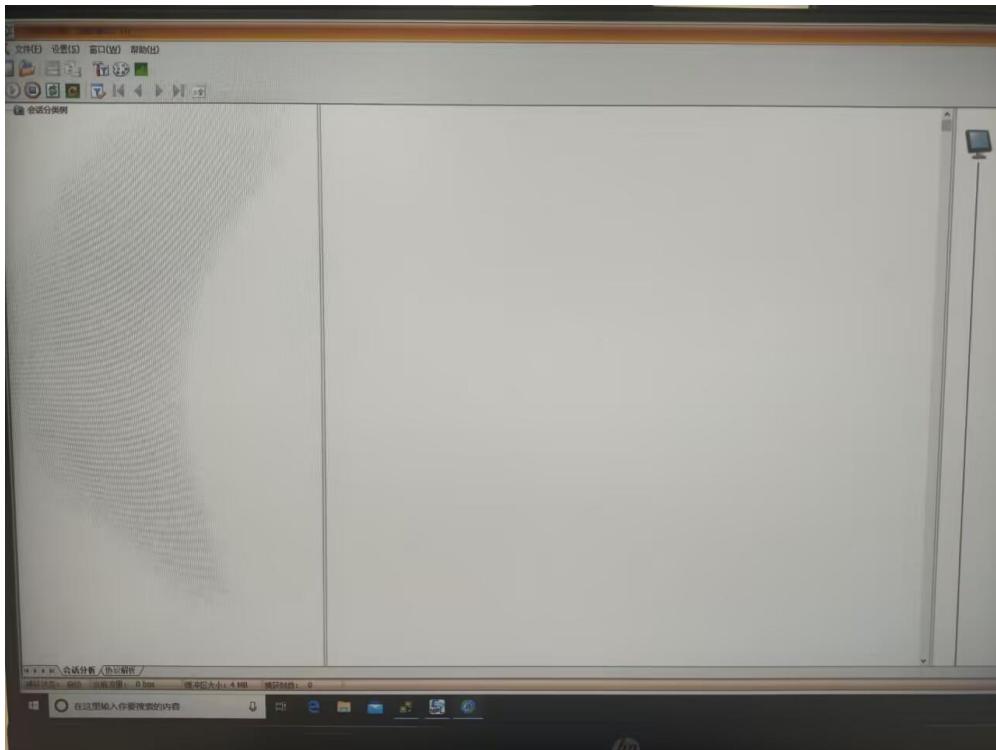
### 练习 1：运行 Ping 命令

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。本练习将主机 A、B、C、D、E、F 作为一组进行实验。实验开始前主机 B 首先执行命令“staticroute\_config”启动静态路由。

1. 主机 B、E、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ICMP 协议）。
  2. 主机 A ping 主机 E (172.16.0.2)。
  3. 主机 B、E、F 停止捕获数据，查看捕获到的数据，并回答以下问题：
- 主机 B 和 E 捕获到的数据如下：



➤ 主机 F 捕获到的数据是空白：



● 捕获的报文对应的“类型”和“代码”字段分别是什么？

答：在 Ping 的过程中，涉及两种 ICMP 报文：回显请求 和 回显应答。

- 回显请求报文 (A 发送给 E):

- 类型 (Type): 8

- 代码 (Code): 0
- 回显应答报文 (E 回复给 A):
  - 类型 (Type): 0
  - 代码 (Code): 0
- 分析报文中的哪些字段保证了回显请求报文和回显应答报文的一一对应?

答: 仅仅靠源 IP 和目的 IP 是不够的 (因为可能同时有多个 Ping 程序在运行)。ICMP 头部中的以下两个字段保证了一一对应:

- ✧ 标识: 用于标识发送回显请求的进程。应答报文会复制请求报文中的 ID, 这样主机 A 收到应答时, 知道是哪个进程 (比如哪个 CMD 窗口) 发起的。
- ✧ 序列号: 用于标识该进程发送的每一个具体的报文。Ping 命令每发送一次, 序列号通常加 1。应答报文也会复制这个序列号, 确保 A 知道收回来的是第几个包。

## 练习 2: ICMP 查询报文

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 主机 A 启动协议编辑器, 编辑一个 ICMP 时间戳请求数据帧发送给主机 C (172.16.1.3)。

MAC 层:

目的 MAC 地址: C 的 MAC 地址。

源 MAC 地址: A 的 MAC 地址。

协议类型或数据长度: 0800。

IP 层:

总长度: 包含 IP 层和 ICMP 层长度。

高层协议类型: 1。

校验和：在其它字段填充完毕后计算并填充。

源 IP 地址：A 的 IP 地址。

目的 IP 地址：C 的 IP 地址。

ICMP 层：

类型：13。

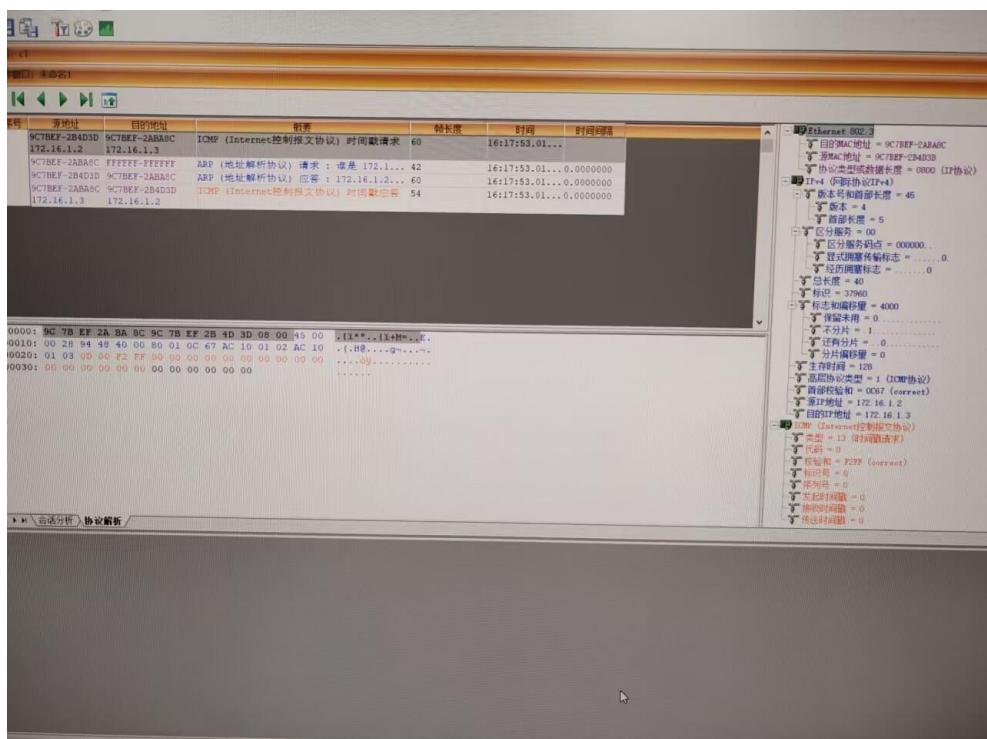
代码字段：0。

校验和：在 ICMP 层其它字段填充完毕后，计算并填充。

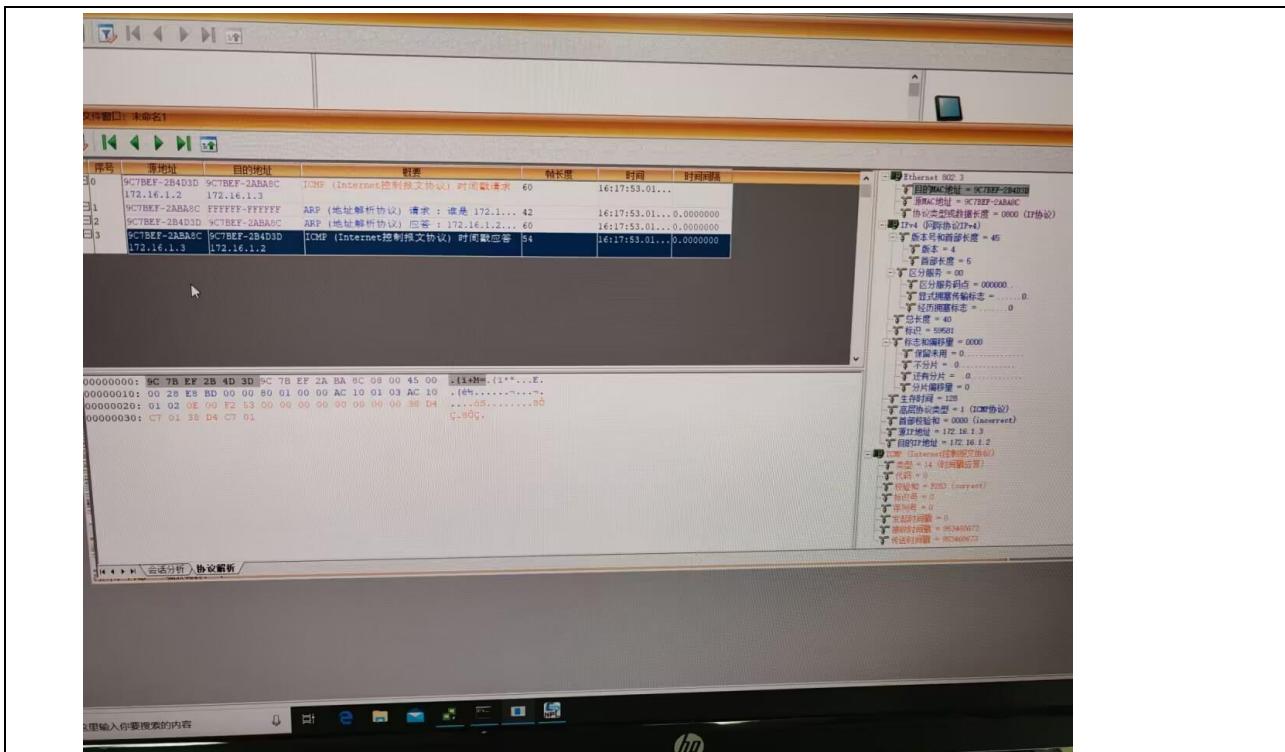
其它字段使用默认值。

2. 主机 C 启动协议分析器进行数据捕获，并设置过滤条件（提取 ICMP 协议）。
3. 主机 A 发送已编辑好的数据帧。
4. 主机 C 停止捕获数据。查看主机 C 捕获到的数据，并填写下表：

➤ 时间戳请求报文：



➤ 时间戳应答报文：



### ● 记录实验结果

时间戳请求报文		时间戳应答报文	
ICMP 字段名	字段值	ICMP 字段名	字段值
类型	13	类型	14
标识号	0	标识号	0
序列号	0	序列号	0
发起时间戳	0	发起时间戳	0
接受时间戳	0	接受时间戳	953468673
传送时间戳	01	传送时间戳	963468673

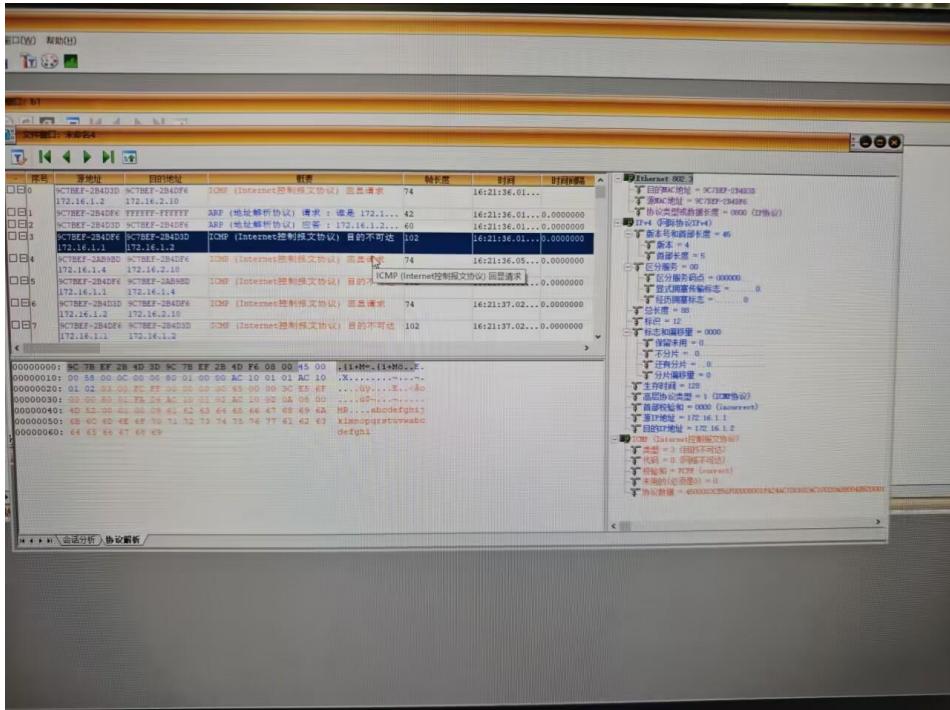
### 练习 3：ICMP 差错报文

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

## 1. 目的端不可达

- (1) 主机 A、B、C、D、E、F 启动协议分析器捕获数据，并设置过滤条件（提取 ICMP）。
- (2) 在主机 A、C、D、E 上 ping 172.16.2.10（不存在的 IP）。
- (3) 主机 A、B、C、D、E、F 停止捕获数据。查看捕获到的数据，并回答以下问题：

➤ 捕获到的数据如下：



● 捕获到的是哪一种目的端不可达报文？

答：属于网络不可达

✧ 现象：路由器完全找不到去往 172.16.2.x 网段的路由条目。

✧ 结果：

- 类型 (Type): 3
- 代码 (Code): 0 (Network Unreachable / 网络不可达)

## 2. 超时

- (1) 在主机 E 上启动协议编辑器，编写一个发送给主机 D (172.16.1.4) 的 ICMP 数据帧。其中：

MAC 层：

目的 MAC 地址：主机 B 的 MAC 地址（172.16.0.1 接口的 MAC）。

源 MAC 地址：E 的 MAC 地址。

协议类型或数据长度：0800。

IP 层：

总长度：包含 IP 层和 ICMP 层长度。

TTL：0。

高层协议类型：1。

校验和：在其它字段填充完毕后，计算并填充。

源 IP 地址：E 的 IP 地址。

目的 IP 地址：D 的 IP 地址。

ICMP 层：

类型：8。

代码字段：0。

校验和：在 ICMP 其它字段填充完毕后，计算并填充。

其它字段使用默认值。

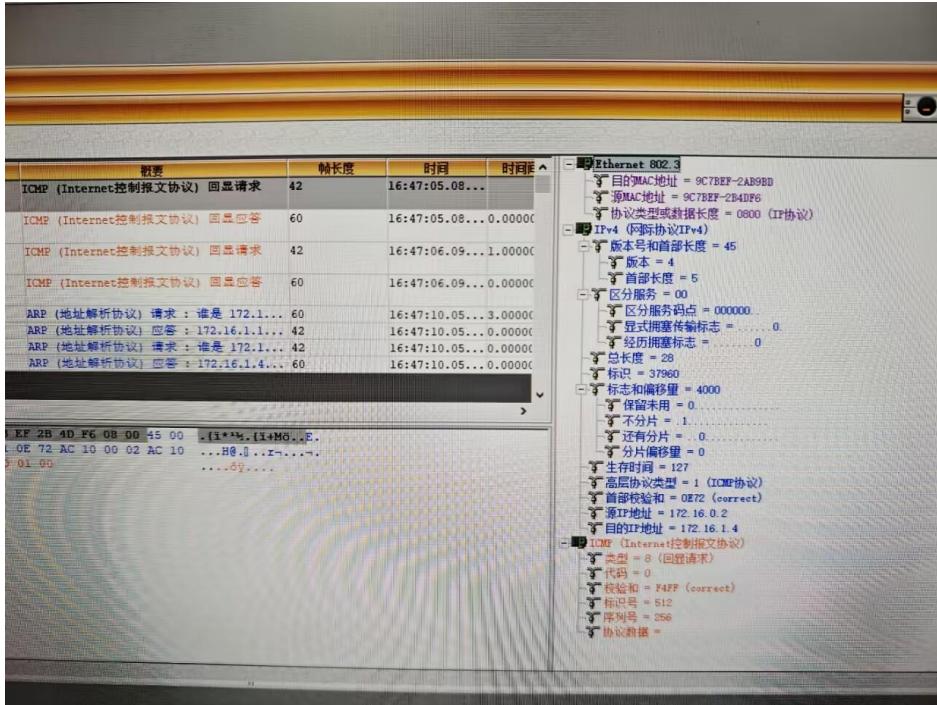
(2) 主机 B(172.16.0.1 的接口)、F 启动协议分析器捕获数据，并设置过滤条件（提取 ICMP 协议）。

(3) 主机 E 发送已编辑好的数据帧。

(4) 主机 B、F 停止捕获数据，查看、记录并分析捕获到的数据。

● 记录实验结果

➤ **主机 B 所收到的结果如下：**



可以看到这里的目的和源 MAC 都分别变成了 D 和 B 的，而并不是 E 一开始编辑的，这也恰恰符合定理。

(5) 主机 B 在命令行方式下输入 recover\_config 命令，停止静态路由服务。

```

:\Users\Administrator>staticroute_config
[SC] ChangeServiceConfig 成功

SERVICE_NAME: remoteaccess
    TYPE               : 20  WIN32_SHARE_PROCESS
    STATE              : 2  START_PENDING
                      (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x7d0
    PID                : 5332
    FLAGS              :

C:\Users\Administrator>recover_config
C:\Users\Administrator>

```

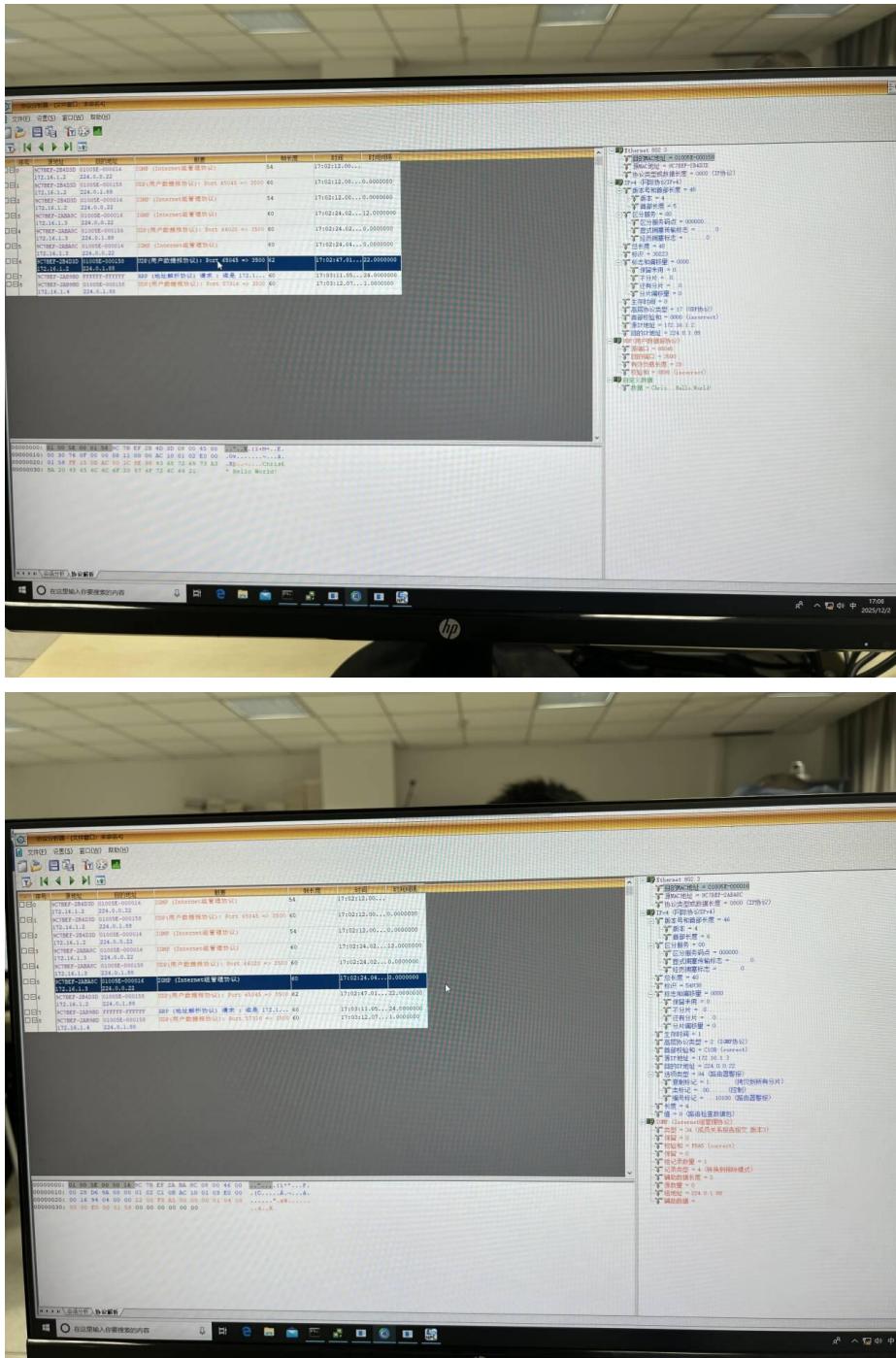
#### 练习 4：利用 IGMP 加入一个多播组

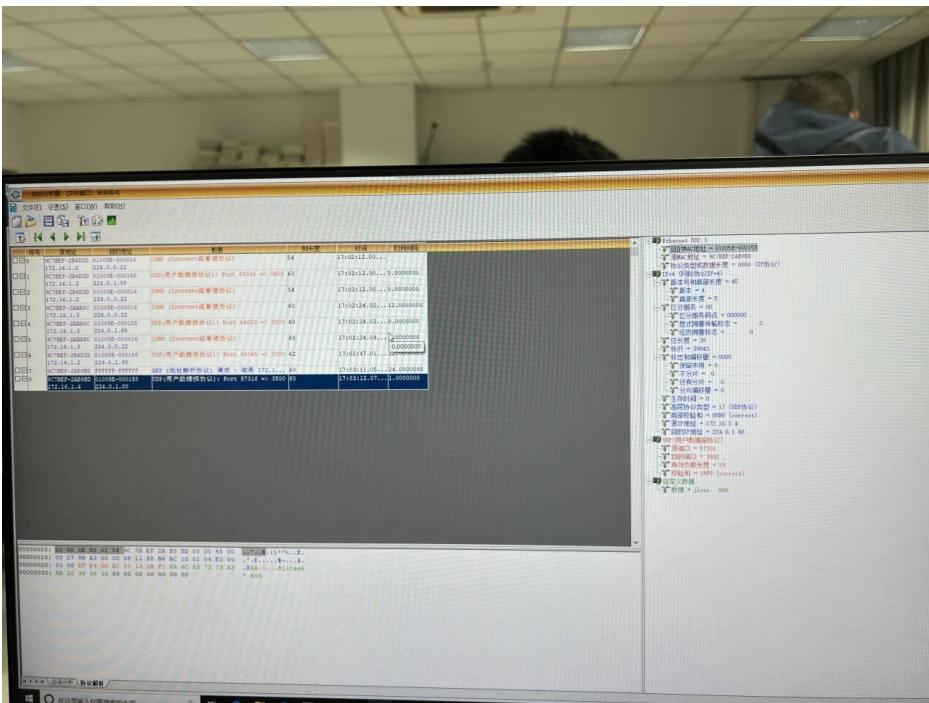
本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 在主机 A、B、C、D、E、F 上启动协议分析器捕获数据，并设置过滤条件（提取 IGMP）。
2. 在主机 A、C、D、E 上启动“组播工具”（方法：实验平台工具栏中的组播工具），并加入多播组（使用 224.0.1.88 作为多播地址）。

3. 在主机 A、B、C、D、E、F 上观察协议分析器上采集到的数据。
  4. 理解“组播工具”使用 IGMP 协议加入一个多播组的过程。
  5. 在主机 A、C、D、E 上点击“离开组播”退出多播组。

➤ 以 A 主机截图为例：





通过协议分析器可以清晰地观察到主机与多播组之间的动态交互。在加入阶段，主机 A/C/D/E 主动发送了目的地址为 224.0.1.88 的 IGMP 报告报文，标志着多播会话的建立。此时，只有加入该组的主机网卡才会接收并处理发往该 IP 的数据帧，未加入的主机（如未操作时的 B、F）则会忽略这些数据。这一现象直观地体现了多播技术“点对多点”传输的特性，即只将数据传送给明确请求加入的接收者，而非整个子网。

### 三、实验总结与收获

通过本次关于 ICMP 和 IGMP 协议的实验，我深入理解了网络层控制报文的工作机制，并熟练掌握了协议分析器和编辑器的使用方法。具体收获如下：

- **深入理解了 ICMP 回显机制 (Ping 原理)：** 通过练习 1，我直观地分析了 Ping 命令背后的 ICMP 回显请求 (Type 8) 与应答 (Type 0) 报文。我明白了在多进程通信中，仅仅依靠 IP 地址是不够的，标识符和序列号字段对于保证请求与应答报文的一一对应至关重要，确保了回显数据能准确返回给发送进程。
- **掌握了网络故障的排查与分析方法：** 在练习 3 的差错报文实验中，我学会了如何根

据 ICMP 报文头部的 **Type** 和 **Code** 字段来判断具体的网络故障。例如，在 Ping 不存在的 IP (172.16.2.10) 时，捕获到了 **Type 3, Code 0** 的报文，这明确指出了“网络不可达”错误，说明路由器无法找到目标网段的路由条目，而非单纯的主机不可达。

- 验证了 **TTL** 机制与路由行为：通过手动构造 TTL=0 的数据包发送给下一跳，我观察到了路由器丢弃该包并返回“超时”报文的过程。同时，观察到捕获的数据帧中源 MAC 地址变为了路由器的接口 MAC，这验证了数据包在经过三层设备转发时，IP 地址保持不变但 MAC 地址逐跳改变的原理。
- 了解了 **IGMP** 组播管理流程：通过练习 4，我实际操作了主机加入和离开多播组 (224.0.1.88) 的过程，并通过分析捕获的 IGMP 数据包，理解了主机如何通过发送成员关系报告来告知路由器其对特定组播组的兴趣，加深了对组播通信原理的认识。

综上所述，本次实验将理论知识与实际抓包分析相结合，不仅让我对 ICMP 和 IGMP 的帧格式有了具象的认知，也提升了我分析底层网络数据和排查网络连通性问题的实践能力。